

Contents

Executive Summary 2

Project Team 2

Project Details..... 2

 Project Purpose 3

 What is Problem Addressed 4

 How is the Problem Addressed 4

Required Resources 4

Deliverables 4

Challenges 6

 Technical Challenges 6

 Non-Technical Challenges 6

Appendices 9

 Teamwork Allocation..... 9

 References & Citations 9

 Installation Documentation10

Executive Summary

This project is centered around enhancing the security of virtualized systems using VMware Security Hardening techniques. The primary goal is to align with business requirements by fortifying system resilience, addressing potential vulnerabilities, and ensuring robust security practices.

The project involves multiple critical tasks, including regular software updates, securing remote access configurations, enforcing strong password policies, and implementing comprehensive monitoring to identify and mitigate threats proactively. These measures aim to create a secure and reliable environment, reducing exposure to cyber risks while improving operational efficiency.

The expected outcomes of this project include a significant reduction in system vulnerabilities, strengthened defense mechanisms, and adherence to industry best practices and compliance standards. By applying these strategies, the project not only protects the infrastructure but also builds a strong foundation for sustainable and secure business operations. This initiative highlights the organization's commitment to maintaining high security standards and ensuring the integrity of its virtualized environments.

Project Team

Mohamad Almasri (101167438):

Skilled in system administration and security practices, contributing knowledge of patching, updates, and security configurations. Brings a focus on project organization and teamwork.

Adeshina Samuel (101501091):

Expertise in configuring firewalls and managing network security. Adds value by ensuring secure connections and system hardening techniques.

Rahul Patel (101378458):

Specialized in automation and unattended updates. Enhances project efficiency by implementing streamlined processes.

Aleksandro Kacorri (101516461):

Experienced in auditing and intrusion detection systems. Contributes to the project by improving monitoring and compliance strategies.

Project Details

Project Purpose:

The purpose of this project is to enhance the security of VMware virtual machines (VMs) by identifying and addressing common vulnerabilities, implementing robust hardening measures, and ensuring alignment with industry-recognized security best practices. Virtual machines are essential components of modern IT infrastructures, but their inherent flexibility and connectivity can also make them targets for potential threats.

This project focuses on closing security gaps by applying a series of proactive and defensive strategies. These include securing remote access protocols, enforcing strong authentication and password policies, configuring firewalls, applying timely updates and patches, and using monitoring tools to detect unusual activities. The goal is to minimize exposure to threats, reduce risks of unauthorized access, and build a resilient, hardened environment that safeguards critical assets.

By implementing these measures, the project not only protects the virtualized systems but also ensures compliance with regulatory and organizational standards, enhancing overall operational integrity and reliability. This initiative reflects a commitment to maintaining a secure, efficient, and future-proof IT infrastructure that supports business continuity.

What is Problem Addressed

VMs are vulnerable to cyberattacks if not properly configured. Weak passwords, open SSH access, and unpatched systems are risks that need addressing.

How is the Problem Addressed

Applying updates and patches.

Securing SSH by disabling root login and changing default ports.

Configuring firewalls, enforcing password policies, and monitoring logs.

Required Resources

Hardware: VMware-compatible systems.

Software: Ubuntu Server/Desktop, VMware Workstation.

Tools: Fail2Ban, AppArmor, auditing tools, MFA applications.

Skills

Required Resources

- **Hardware:** VMware-compatible systems.
- **Software:** Ubuntu Server/Desktop, VMware Workstation.
- **Tools:** Fail2Ban, AppArmor, auditing tools, MFA applications.
- **Skills:** Security hardening, system monitoring, vulnerability detection.

Deliverables

This project aims to produce the following comprehensive deliverables:

Secured Virtual Machines (VMs)

Fully configured and hardened Ubuntu Desktop VMs with applied security measures.

Implementation of robust firewall settings, SSH hardening, and strong authentication policies.

Detailed Documentation

- A step-by-step installation and configuration guide for all hardening measures, including screenshots and command references.

Reports on identified vulnerabilities and the corresponding solutions implemented.

- Automated Update Mechanism

A fully functional unattended-upgrades system to ensure timely application of critical patches without manual intervention.

- Vulnerability Scan Report

Results from tools like Nessus, Lynis, or Fail2Ban, showing identified vulnerabilities and proof of resolution.

- Monitoring and Auditing Logs

Comprehensive system activity logs demonstrating the successful implementation of monitoring tools like auditd and Logwatch.

- AppArmor Configuration

Customized profiles ensuring applications run securely within defined boundaries.

- Multi-Factor Authentication (MFA)

Integration of MFA for SSH access, showcasing additional layers of security beyond traditional password authentication.

- Team Contributions Summary

Clear documentation of each team member's role, contributions, and tasks completed throughout the project.

- Compliance with Best Practices

A final review and checklist demonstrating adherence to VMware and Ubuntu security hardening guidelines.

- Technical Presentation

A formal presentation summarizing the project's objectives, methodology, and results, suitable for technical stakeholders.

Challenges

Technical Challenges

1. Challenge: SSH Security Vulnerabilities

Explanation:

The default SSH configuration (port 22 and root login enabled) is a common target for brute-force and unauthorized access attempts. This posed a significant risk to system security.

Work-Around:

Disabled root login in the SSH configuration file (`/etc/ssh/sshd_config`).

Changed the default port to a non-standard port, such as 2222.

Enabled Fail2Ban to monitor and block repeated unauthorized login attempts.

2. Challenge: Configuring a Firewall with UFW

Explanation:

Setting up a firewall using UFW (Uncomplicated Firewall) to allow only necessary connections while blocking unauthorized traffic was tricky due to ensuring no essential services were inadvertently blocked.

Work-Around:

Carefully reviewed system requirements to identify necessary ports (SSH, HTTP).

Allowed essential traffic while denying all other connections.

3. Challenge: Enforcing Strong Password Policies

Explanation:

By default, there were no strict password requirements, which could allow users to set weak passwords, increasing the risk of unauthorized access.

Work-Around:

Installed and configured libpam-pwquality to enforce minimum password length, complexity, and history.

Educated team members on the importance of strong passwords.

Non-Technical Challenges

1. Challenge: Team Coordination

Explanation:

With team members having different schedules and availability, aligning work sessions and ensuring consistent communication was difficult. This caused delays in task completion and misunderstandings about responsibilities.

Solution:

Established a shared calendar to plan meetings and deadlines.

Used collaboration tools like Microsoft Teams and Google Docs to communicate and work asynchronously.

Conducted weekly check-ins to track progress and address issues.

2. Challenge: Managing Time and Deadlines

Explanation:

Balancing this project with other academic and personal responsibilities made it challenging for some members to meet deadlines. This resulted in last-minute work and increased stress levels.

Solution:

Broke the project into smaller milestones with clear deadlines.

Assigned tasks with realistic timelines based on each member's availability.

Prioritized critical components first to ensure the project remained on

Appendices

Teamwork Allocation

Mohamad Almasri:

Completed all the reports and performed the system installations, ensuring detailed documentation, screenshots, and proper configuration of the system.

Adeshina Samuel:

Took primary responsibility for auditing tasks and verifying system compliance and configurations.

Rahul Patel:

Designed and prepared the PowerPoint presentation, ensuring the project's key findings and results were effectively presented.

Aleksandro Kacorri:

Took primary responsibility for auditing tasks and verifying system compliance and configurations.

References & Citations

VMware Security Hardening Guidelines.

<https://www.vmware.com/solutions/security/hardening-guides>

Ubuntu Security Documentation.

<https://ubuntu.com/security/certifications/docs/usg>

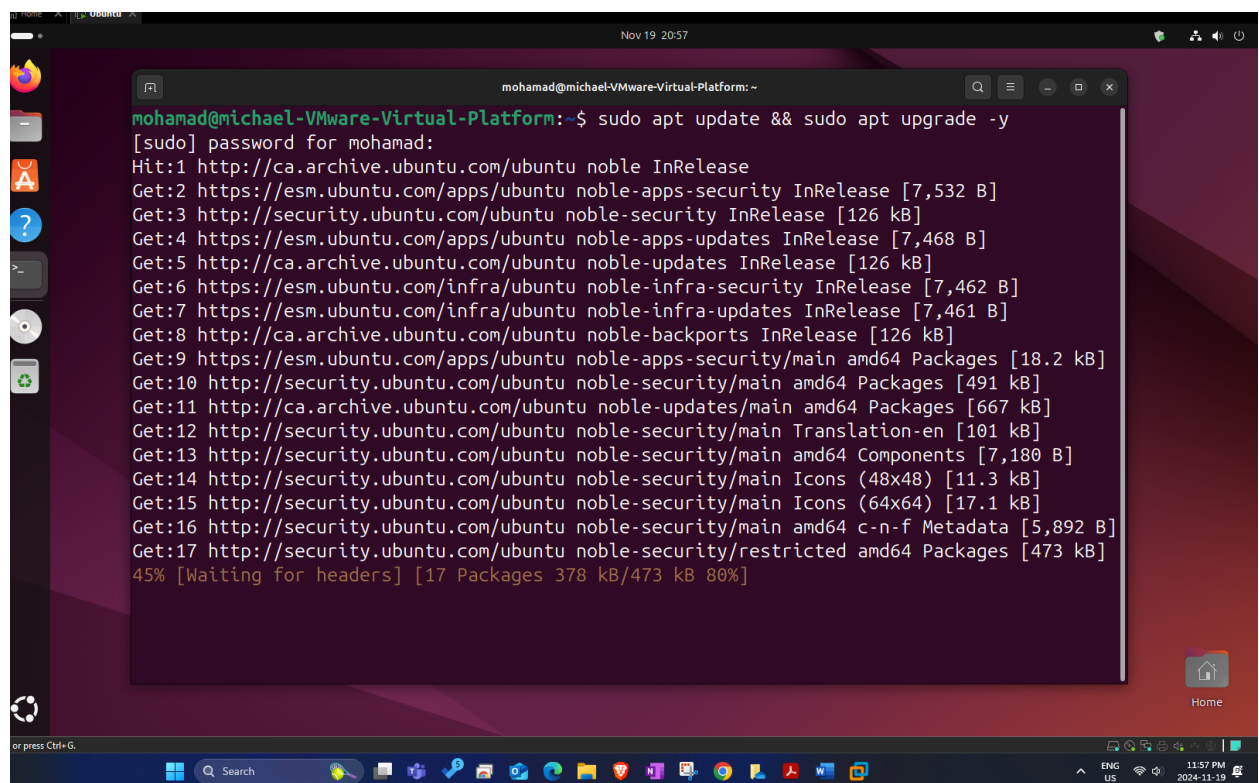
Installation Documentation

Update and Patch the System

Keep software up-to-date:

Run regular updates to ensure all security patches are applied

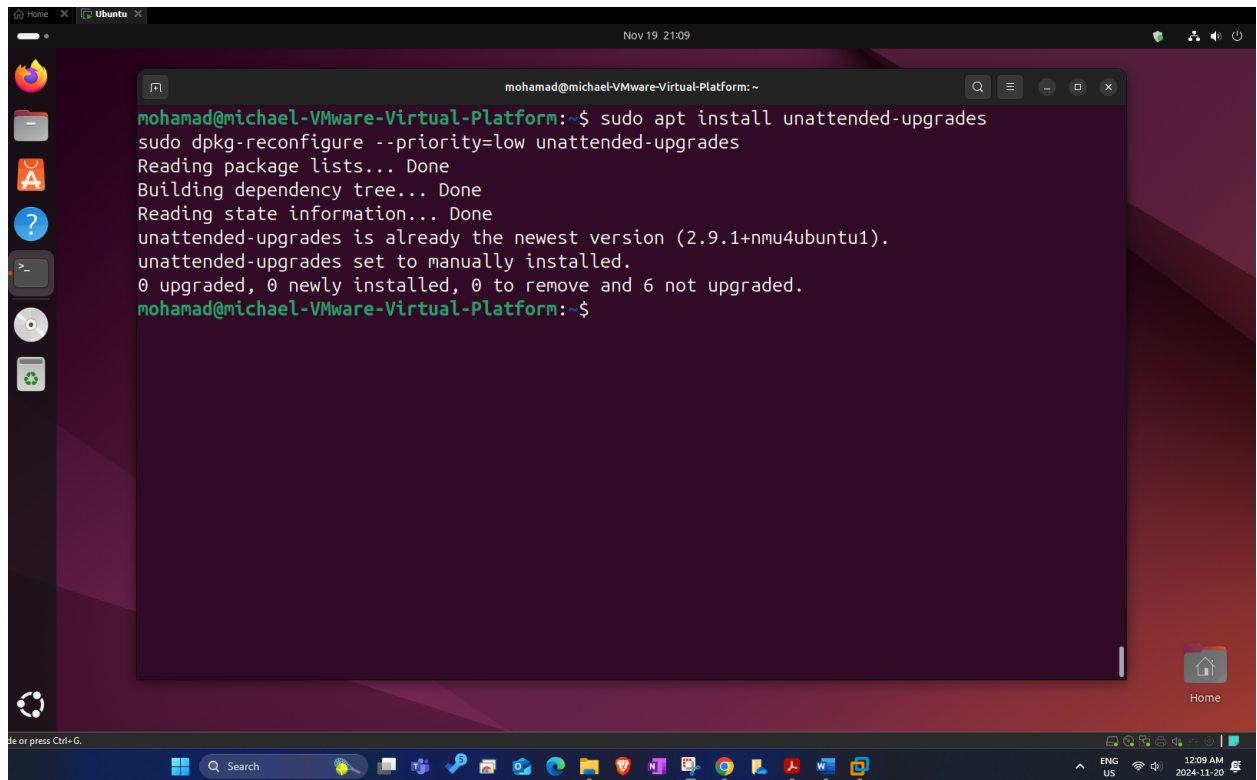
```
sudo apt update && sudo apt upgrade -y
```



```
mohamad@michael-VMware-Virtual-Platform: ~  
mohamad@michael-VMware-Virtual-Platform:~$ sudo apt update && sudo apt upgrade -y  
[sudo] password for mohamad:  
Hit:1 http://ca.archive.ubuntu.com/ubuntu noble InRelease  
Get:2 https://esm.ubuntu.com/apps/ubuntu noble-apps-security InRelease [7,532 B]  
Get:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]  
Get:4 https://esm.ubuntu.com/apps/ubuntu noble-apps-updates InRelease [7,468 B]  
Get:5 http://ca.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]  
Get:6 https://esm.ubuntu.com/infra/ubuntu noble-infrastructure InRelease [7,462 B]  
Get:7 https://esm.ubuntu.com/infra/ubuntu noble-infrastructure-updates InRelease [7,461 B]  
Get:8 http://ca.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]  
Get:9 https://esm.ubuntu.com/apps/ubuntu noble-apps-security/main amd64 Packages [18.2 kB]  
Get:10 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [491 kB]  
Get:11 http://ca.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [667 kB]  
Get:12 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [101 kB]  
Get:13 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7,180 B]  
Get:14 http://security.ubuntu.com/ubuntu noble-security/main Icons (48x48) [11.3 kB]  
Get:15 http://security.ubuntu.com/ubuntu noble-security/main Icons (64x64) [17.1 kB]  
Get:16 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [5,892 B]  
Get:17 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [473 kB]  
45% [Waiting for headers] [17 Packages 378 kB/473 kB 80%]
```

Enable unattended upgrades:

Automate updates for critical security patches:



The screenshot shows a terminal window titled 'mohamad@michael-VMware-Virtual-Platform: ~' with a search icon, menu icon, and window control buttons. The terminal output is as follows:

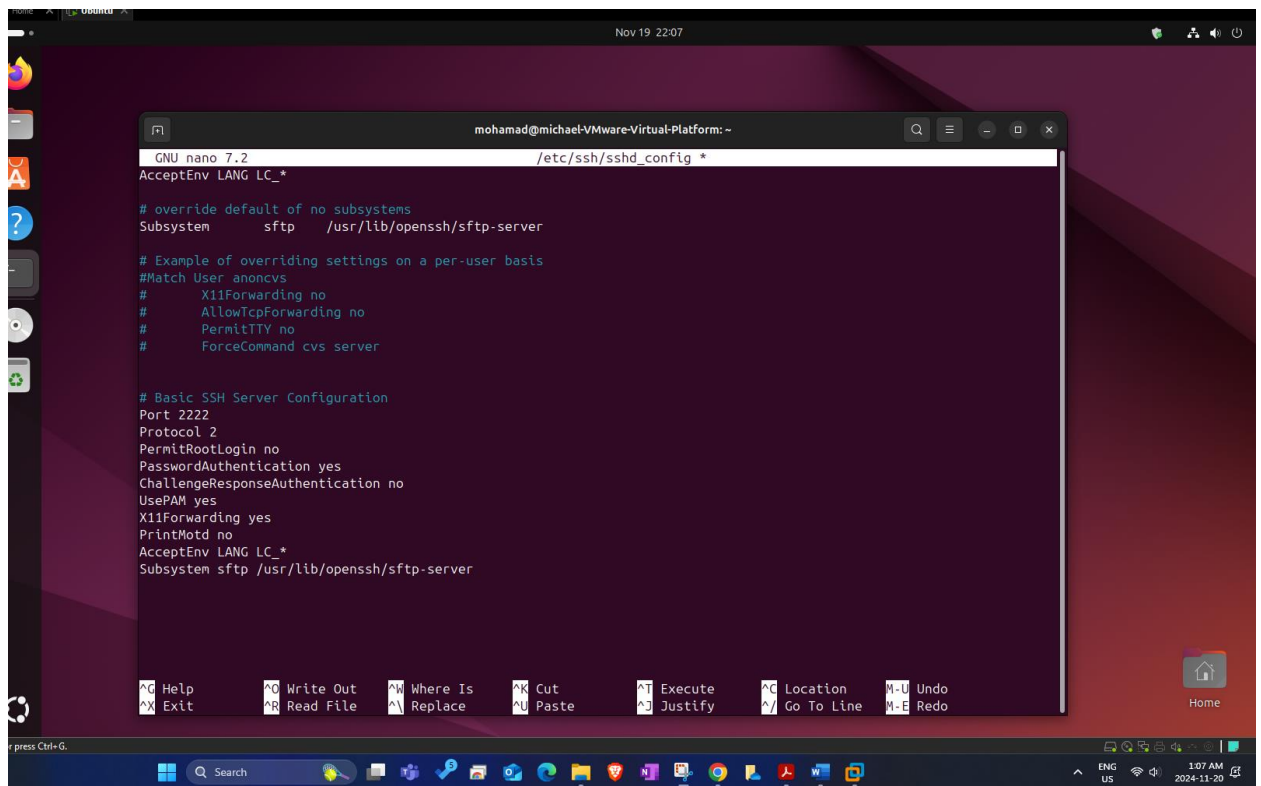
```
mohamad@michael-VMware-Virtual-Platform:~$ sudo apt install unattended-upgrades
sudo dpkg-reconfigure --priority=low unattended-upgrades
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unattended-upgrades is already the newest version (2.9.1+nmu4ubuntu1).
unattended-upgrades set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
mohamad@michael-VMware-Virtual-Platform:~$
```

The terminal is running on an Ubuntu desktop environment. The desktop has a dark purple background with a sidebar on the left containing icons for Firefox, Files, Applications, Help, Terminal, and a disk icon. The bottom of the screen shows a Windows taskbar with a search bar, various application icons, and system status indicators on the right including 'ENG US', signal strength, and the time '12:09 AM 2024-11-20'.

Secure SSH:

Securing SSH (Secure Shell) is a critical step to protect your system from unauthorized access and potential cyberattacks. SSH is a widely used protocol for securely accessing and managing remote systems, but its default settings can make it a target for attackers.

Disable root login:



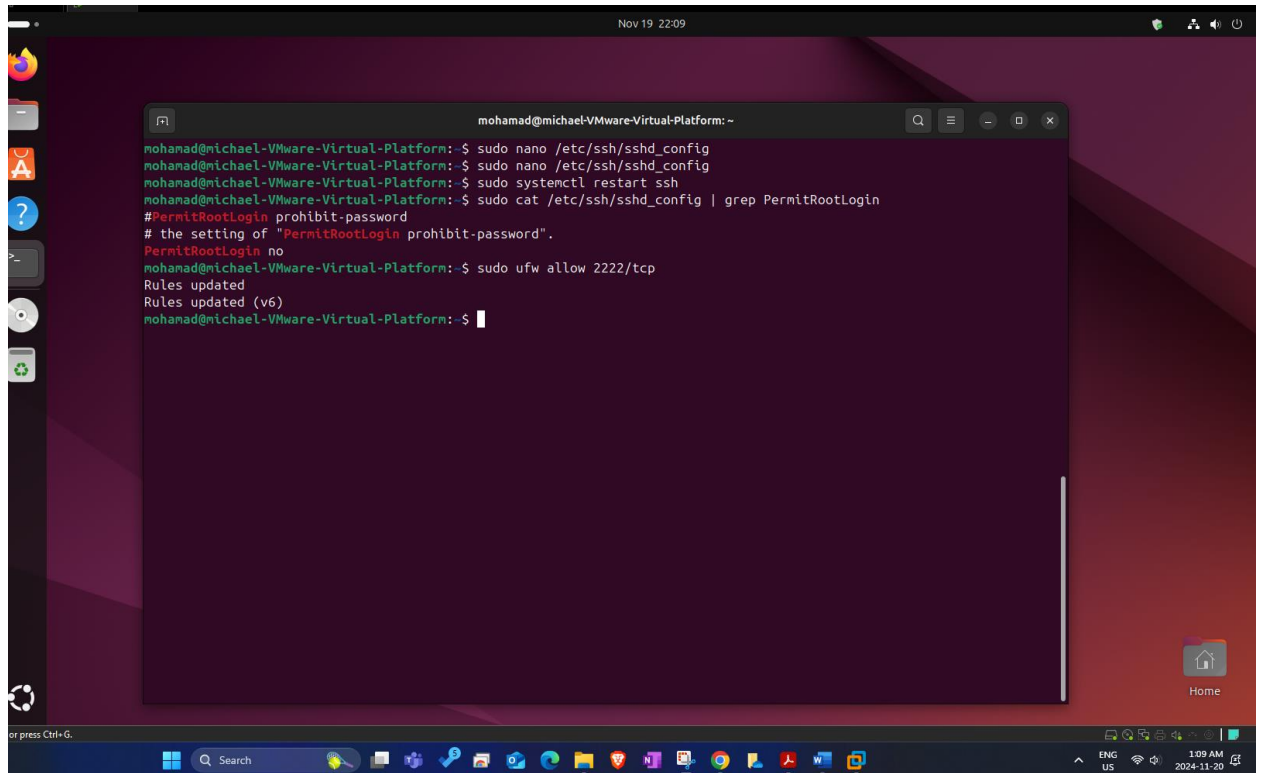
```
GNU nano 7.2 /etc/ssh/sshd_config *
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server

# Basic SSH Server Configuration
Port 2222
Protocol 2
PermitRootLogin no
PasswordAuthentication yes
ChallengeResponseAuthentication no
UsePAM yes
X11Forwarding yes
PrintMotd no
AcceptEnv LANG LC_*
Subsystem sftp /usr/lib/openssh/sftp-server
```

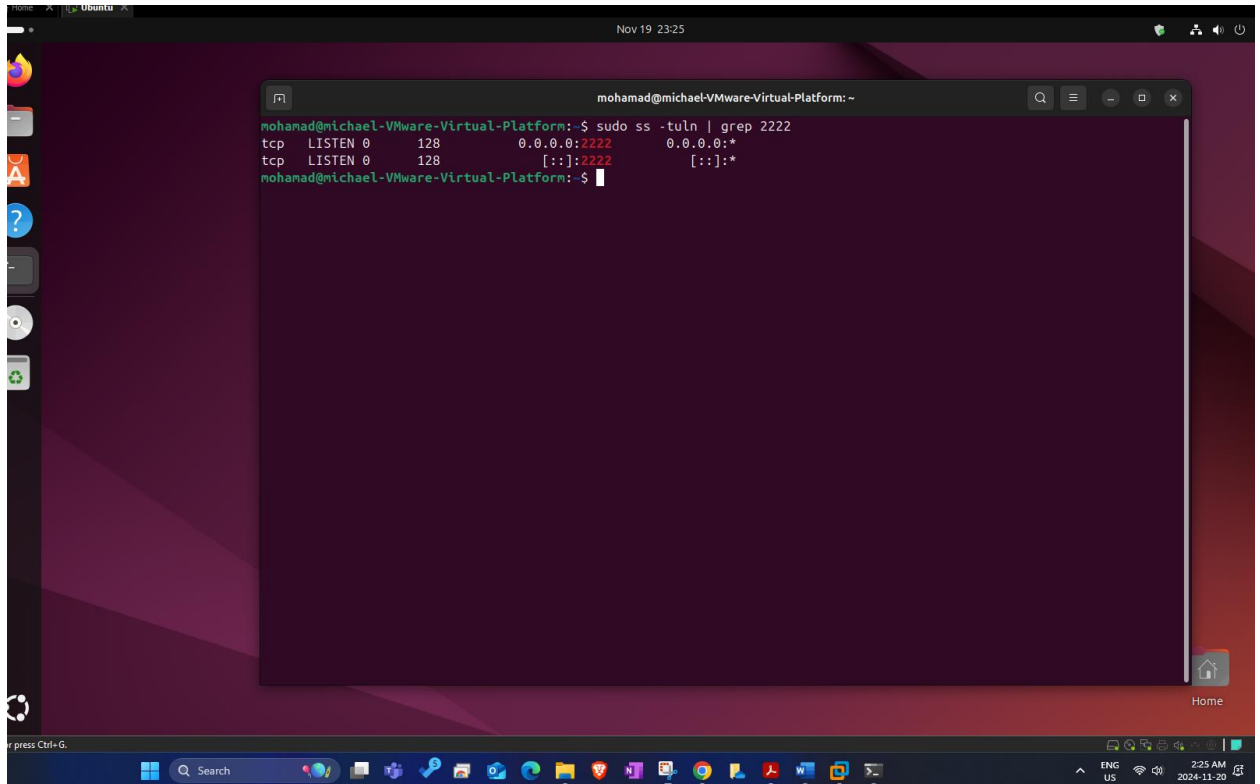
The screenshot shows a terminal window within a VMware virtual machine. The terminal is running the nano text editor, editing the file /etc/ssh/sshd_config. The configuration includes settings for subsystems, user matching, and basic server configuration. The terminal window is titled 'mohamad@michael-VMware-Virtual-Platform: ~'. The VMware interface shows the date 'Nov 19 22:07' and a 'Home' button in the bottom right corner. The bottom of the screen displays a Windows taskbar with various application icons and the system clock showing '1:07 AM 2024-11-20'.



The screenshot shows a terminal window titled "mohamad@michael-VMware-Virtual-Platform: ~" with the following commands and output:

```
mohamad@michael-VMware-Virtual-Platform:~$ sudo nano /etc/ssh/sshd_config
mohamad@michael-VMware-Virtual-Platform:~$ sudo nano /etc/ssh/sshd_config
mohamad@michael-VMware-Virtual-Platform:~$ sudo systemctl restart ssh
mohamad@michael-VMware-Virtual-Platform:~$ sudo cat /etc/ssh/sshd_config | grep PermitRootLogin
#PermitRootLogin prohibit-password
# the setting of "PermitRootLogin prohibit-password".
PermitRootLogin no
mohamad@michael-VMware-Virtual-Platform:~$ sudo ufw allow 2222/tcp
Rules updated
Rules updated (v6)
mohamad@michael-VMware-Virtual-Platform:~$
```

The terminal window is open on a desktop environment with a dark purple background. The desktop has a sidebar on the left with icons for applications like Firefox, LibreOffice, and a help icon. The bottom of the screen shows a Windows taskbar with various application icons and system status indicators on the right, including the time 1:09 AM and date 2024-11-20.



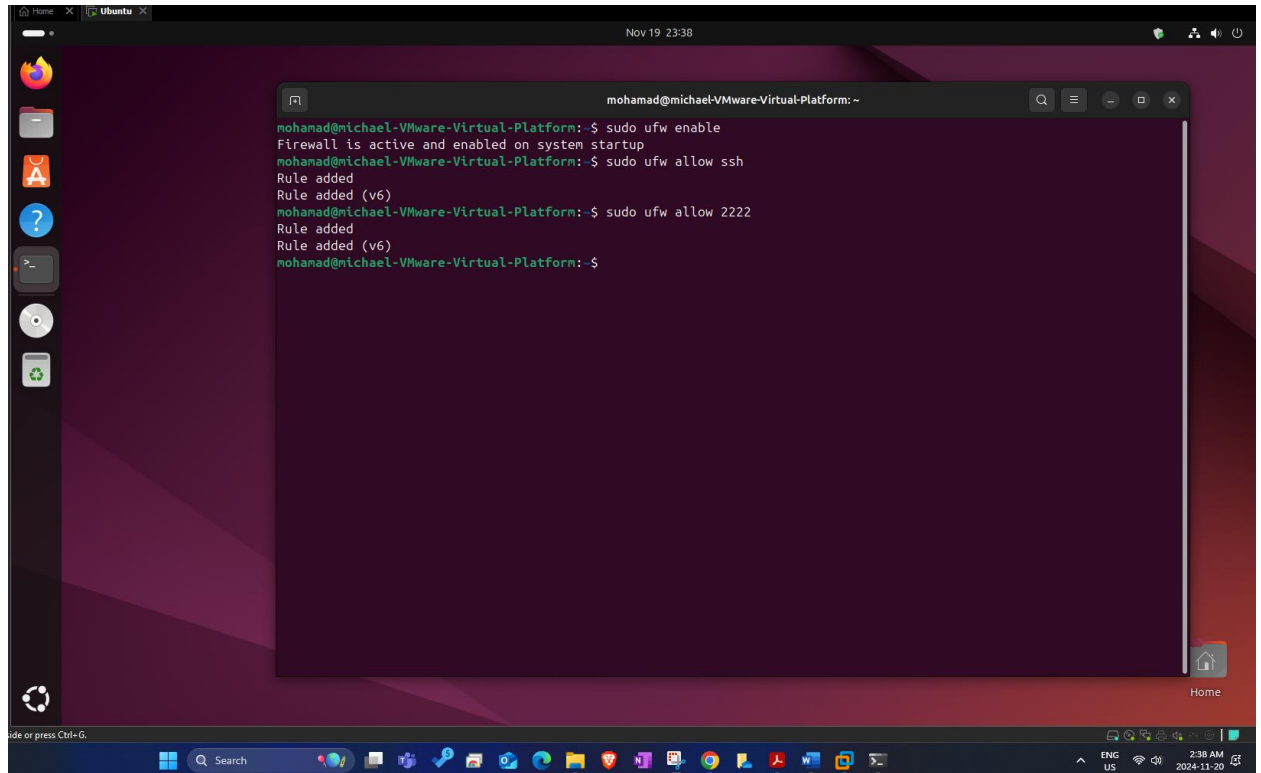
The screenshot shows a terminal window titled 'mohamad@michael-VMware-Virtual-Platform: ~' with a search icon, menu icon, and window control buttons. The terminal output is as follows:

```
mohamad@michael-VMware-Virtual-Platform:~$ sudo ss -tln | grep 2222
tcp    LISTEN 0      128          0.0.0.0:2222  0.0.0.0:*
tcp    LISTEN 0      128          [::]:2222   [::]:*
```

The terminal window is open on a desktop environment with a dark purple background. The desktop has a sidebar on the left with icons for Firefox, LibreOffice, and other applications. The bottom of the screen shows a Windows taskbar with various application icons and system status indicators on the right, including language (ENG US), time (2:25 AM), and date (2024-11-20).

Configure a Firewall

- **Benefit:** Controls which connections are allowed to the system, reducing exposure to attacks.



The screenshot shows a terminal window titled 'mohamad@michael-VMware-Virtual-Platform: ~' running on an Ubuntu desktop. The terminal displays the following commands and output:

```
mohamad@michael-VMware-Virtual-Platform:~$ sudo ufw enable
Firewall is active and enabled on system startup
mohamad@michael-VMware-Virtual-Platform:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
mohamad@michael-VMware-Virtual-Platform:~$ sudo ufw allow 2222
Rule added
Rule added (v6)
mohamad@michael-VMware-Virtual-Platform:~$
```

The desktop background is Ubuntu's default purple and red gradient. The terminal window is a standard Ubuntu terminal with a dark background and light text. The desktop environment includes a sidebar with application icons (Dash, Home, Files, Firefox, LibreOffice, etc.) and a bottom dock with various application shortcuts.

Use Strong Password Policies

- **Benefit:** Prevents weak passwords, reducing the risk of unauthorized access.

```

Note added (18)
mohamad@michael-VMware-Virtual-Platform:~$ sudo apt install libpam-pwquality
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libpam-pwquality is already the newest version (1.4.5-3build1).
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.
mohamad@michael-VMware-Virtual-Platform:~$

```

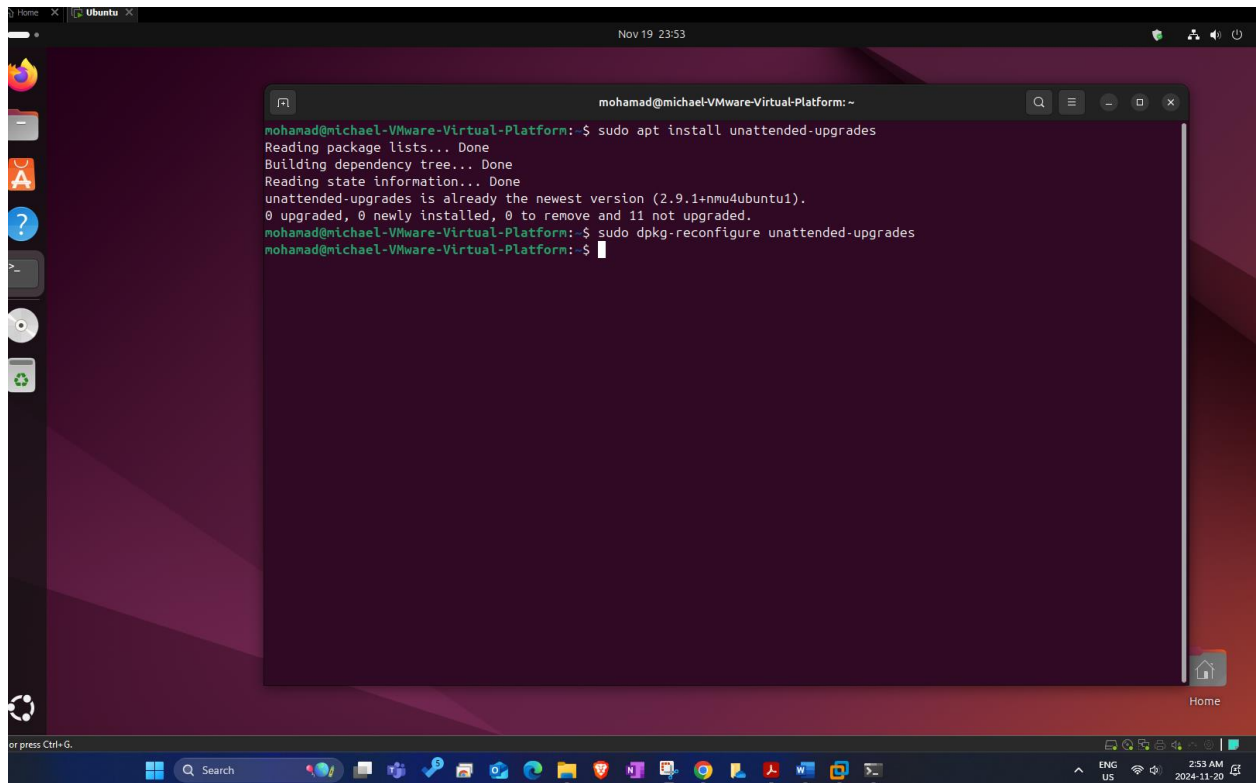
```

GNU nano 7.2 /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
# minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 0
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 0
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.

```


Enable Automatic Security Updates

- **Benefit:** Automatically installs critical updates to keep the system secure without manual intervention.

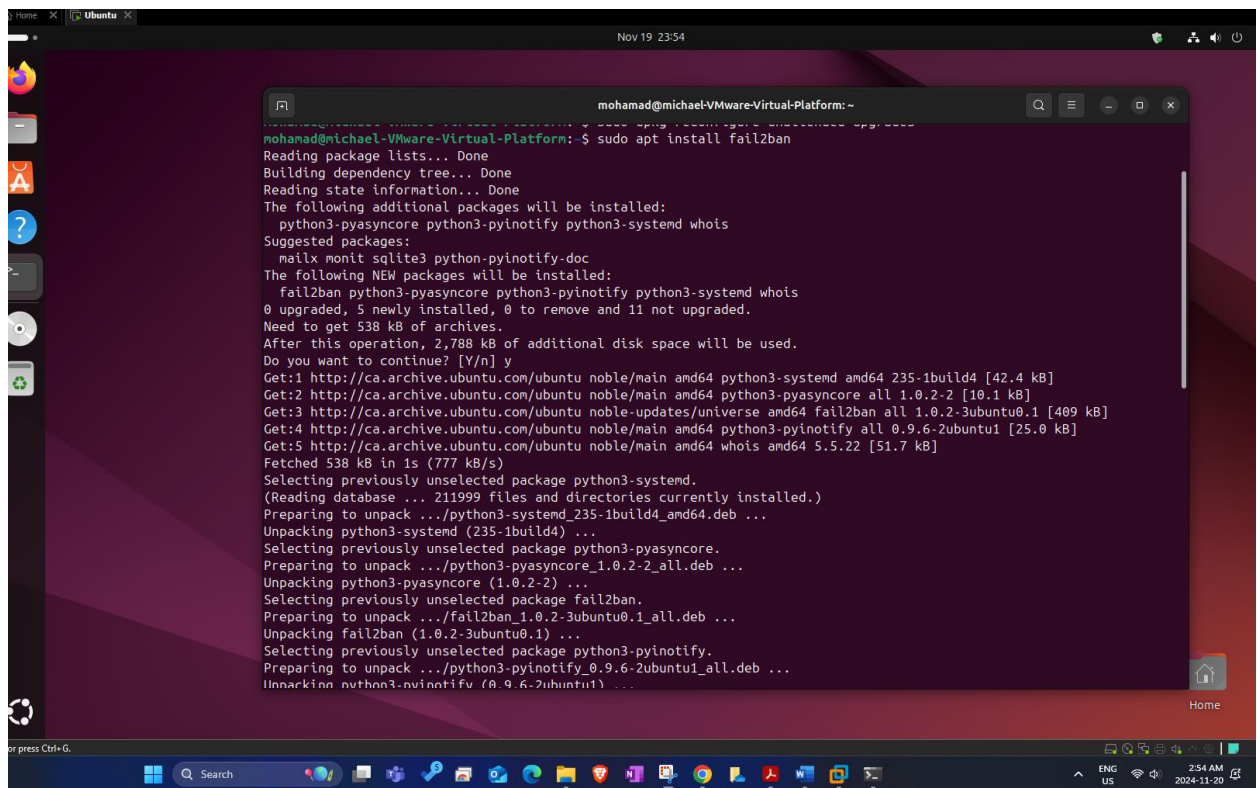


The screenshot shows a terminal window titled 'mohamad@michael-VMware-Virtual-Platform: ~' running on an Ubuntu desktop. The terminal output shows the command 'sudo apt install unattended-upgrades' being executed. The output indicates that the package is already the newest version (2.9.1+nm4ubuntu1) and that no packages need to be upgraded. The prompt then shows 'sudo dpkg-reconfigure unattended-upgrades' being executed, followed by another prompt.

```
mohamad@michael-VMware-Virtual-Platform: ~  
mohamad@michael-VMware-Virtual-Platform: $ sudo apt install unattended-upgrades  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
unattended-upgrades is already the newest version (2.9.1+nm4ubuntu1).  
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.  
mohamad@michael-VMware-Virtual-Platform: $ sudo dpkg-reconfigure unattended-upgrades  
mohamad@michael-VMware-Virtual-Platform: $
```

Use Fail2Ban for Brute-Force Protection

Benefit: Protects the system from repeated unauthorized login attempts by blocking attackers.



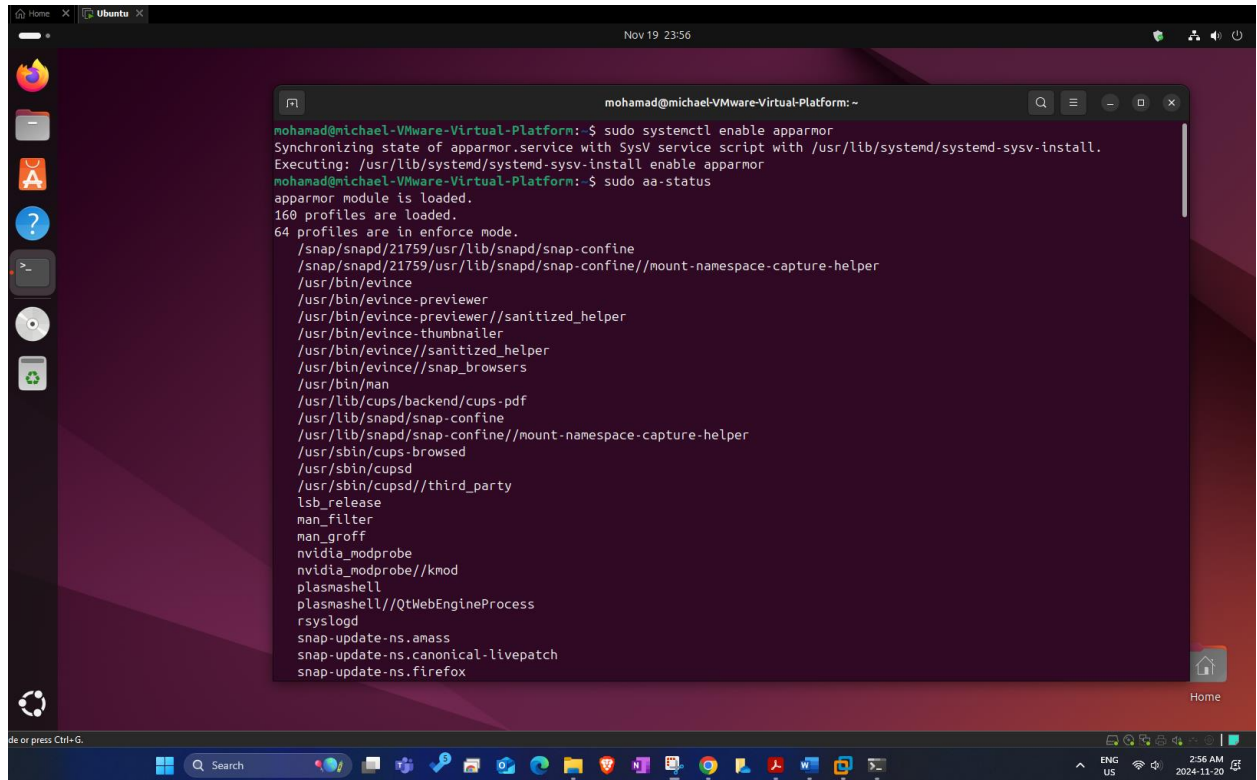
```
mohamad@michael-VMware-Virtual-Platform: ~  
mohamad@michael-VMware-Virtual-Platform:~$ sudo apt install fail2ban  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  python3-pyasyncore python3-pyinotify python3-systemd whois  
Suggested packages:  
  mailx monit sqlite3 python-pyinotify-doc  
The following NEW packages will be installed:  
  fail2ban python3-pyasyncore python3-pyinotify python3-systemd whois  
0 upgraded, 5 newly installed, 0 to remove and 11 not upgraded.  
Need to get 538 kB of archives.  
After this operation, 2,788 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 python3-systemd amd64 235-1build4 [42.4 kB]  
Get:2 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyasyncore all 1.0.2-2 [10.1 kB]  
Get:3 http://ca.archive.ubuntu.com/ubuntu noble-updates/universe amd64 fail2ban all 1.0.2-3ubuntu0.1 [409 kB]  
Get:4 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyinotify all 0.9.6-2ubuntu1 [25.0 kB]  
Get:5 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 whois amd64 5.5.22 [51.7 kB]  
Fetched 538 kB in 1s (777 kB/s)  
Selecting previously unselected package python3-systemd.  
(Reading database ... 211999 files and directories currently installed.)  
Preparing to unpack .../python3-systemd_235-1build4_amd64.deb ...  
Unpacking python3-systemd (235-1build4) ...  
Selecting previously unselected package python3-pyasyncore.  
Preparing to unpack .../python3-pyasyncore_1.0.2-2_all.deb ...  
Unpacking python3-pyasyncore (1.0.2-2) ...  
Selecting previously unselected package fail2ban.  
Preparing to unpack .../fail2ban_1.0.2-3ubuntu0.1_all.deb ...  
Unpacking fail2ban (1.0.2-3ubuntu0.1) ...  
Selecting previously unselected package python3-pyinotify.  
Preparing to unpack .../python3-pyinotify_0.9.6-2ubuntu1_all.deb ...  
Unpacking python3-pyinotify (0.9.6-2ubuntu1) ...
```

Secure Shared Files and Folders

Benefit: Protects sensitive files by restricting access to authorized users only.

Configure AppArmor

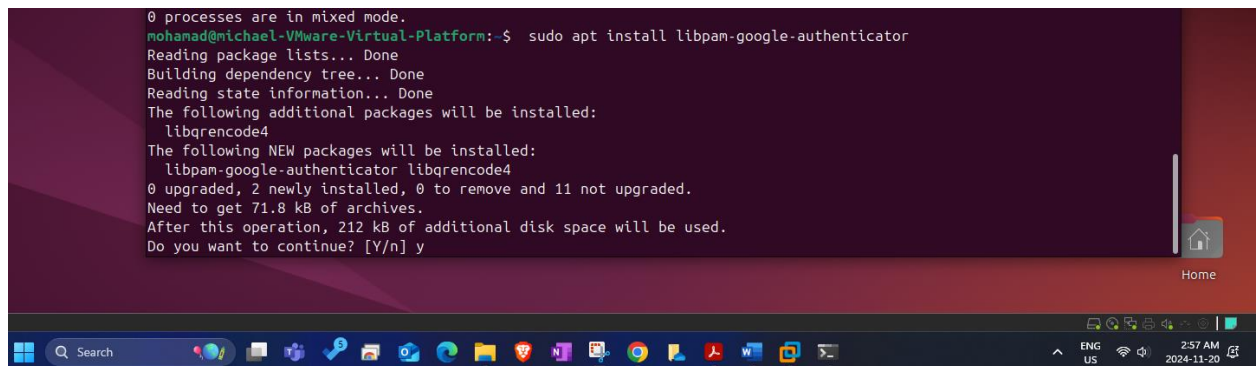
- **Benefit:** Adds extra security by limiting what applications can access on the system.



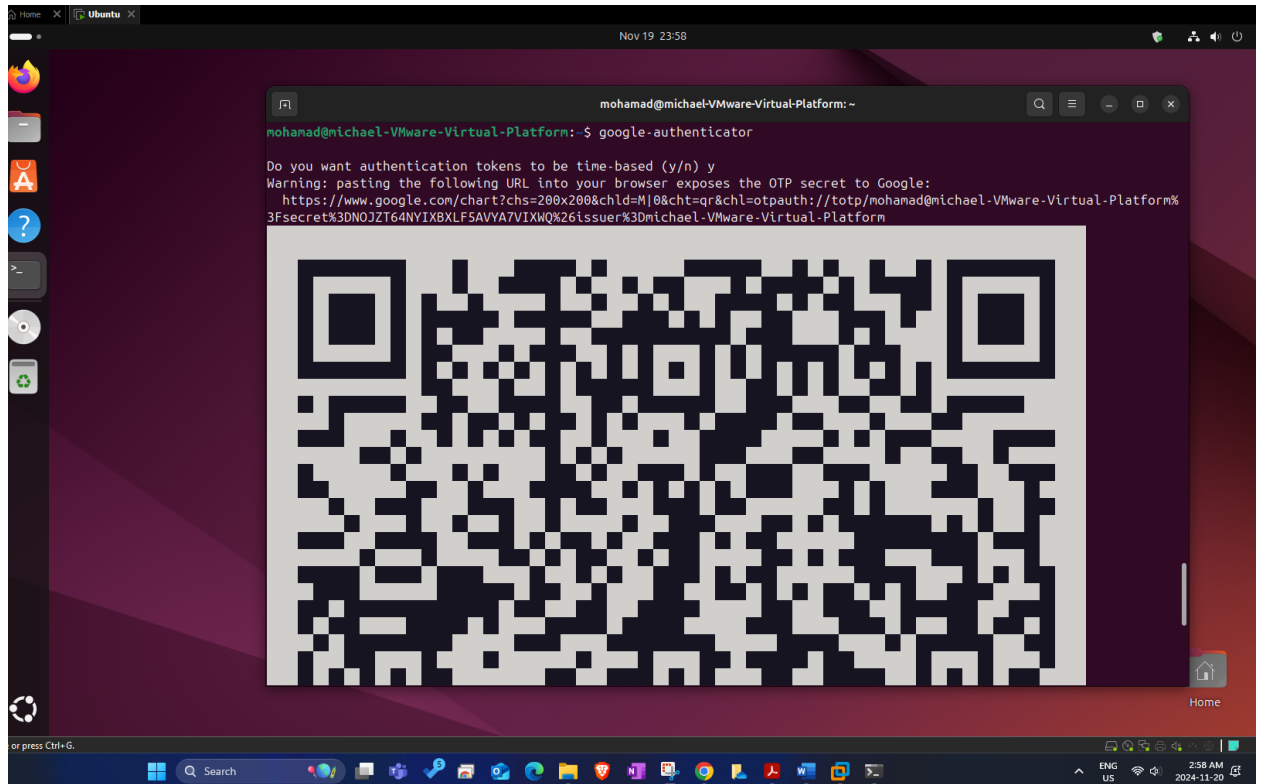
```
mohamad@michael-VMware-Virtual-Platform: ~  
$ sudo systemctl enable apparmor  
Synchronizing state of apparmor.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable apparmor  
mohamad@michael-VMware-Virtual-Platform: ~$ sudo aa-status  
apparmor module is loaded.  
160 profiles are loaded.  
64 profiles are in enforce mode.  
/snap/snapd/21759/usr/lib/snapd/snap-confine  
/snap/snapd/21759/usr/lib/snapd/snap-confine//mount-namespace-capture-helper  
/usr/bin/evince  
/usr/bin/evince-preview  
/usr/bin/evince-preview//sanitized_helper  
/usr/bin/evince-thumbnailer  
/usr/bin/evince//sanitized_helper  
/usr/bin/evince//snap_browsers  
/usr/bin/man  
/usr/lib/cups/backend/cups-pdf  
/usr/lib/snapd/snap-confine  
/usr/lib/snapd/snap-confine//mount-namespace-capture-helper  
/usr/sbin/cups-browsed  
/usr/sbin/cupsd  
/usr/sbin/cupsd//third_party  
lsb_release  
man_filter  
man_groff  
nvidia_modprobe  
nvidia_modprobe//knod  
plasmashell  
plasmashell//QtWebEngineProcess  
rsyslogd  
snap-update-ns.amass  
snap-update-ns.canonical-livepatch  
snap-update-ns.firefox
```

Use Multi-Factor Authentication (MFA)

- **Benefit:** Adds an extra layer of security beyond just a password.

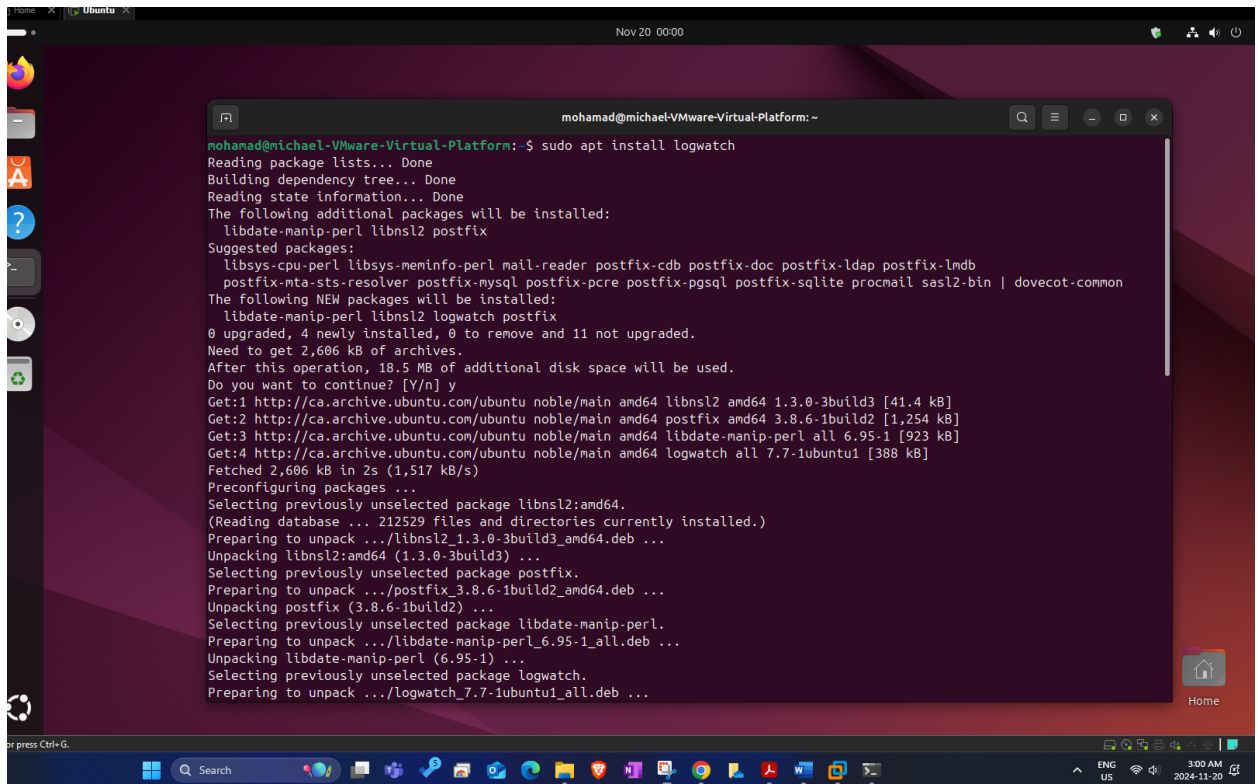


```
0 processes are in mixed mode.  
mohamad@michael-VMware-Virtual-Platform: ~$ sudo apt install libpam-google-authenticator  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  libqrencode4  
The following NEW packages will be installed:  
  libpam-google-authenticator libqrencode4  
0 upgraded, 2 newly installed, 0 to remove and 11 not upgraded.  
Need to get 71.8 kB of archives.  
After this operation, 212 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y
```

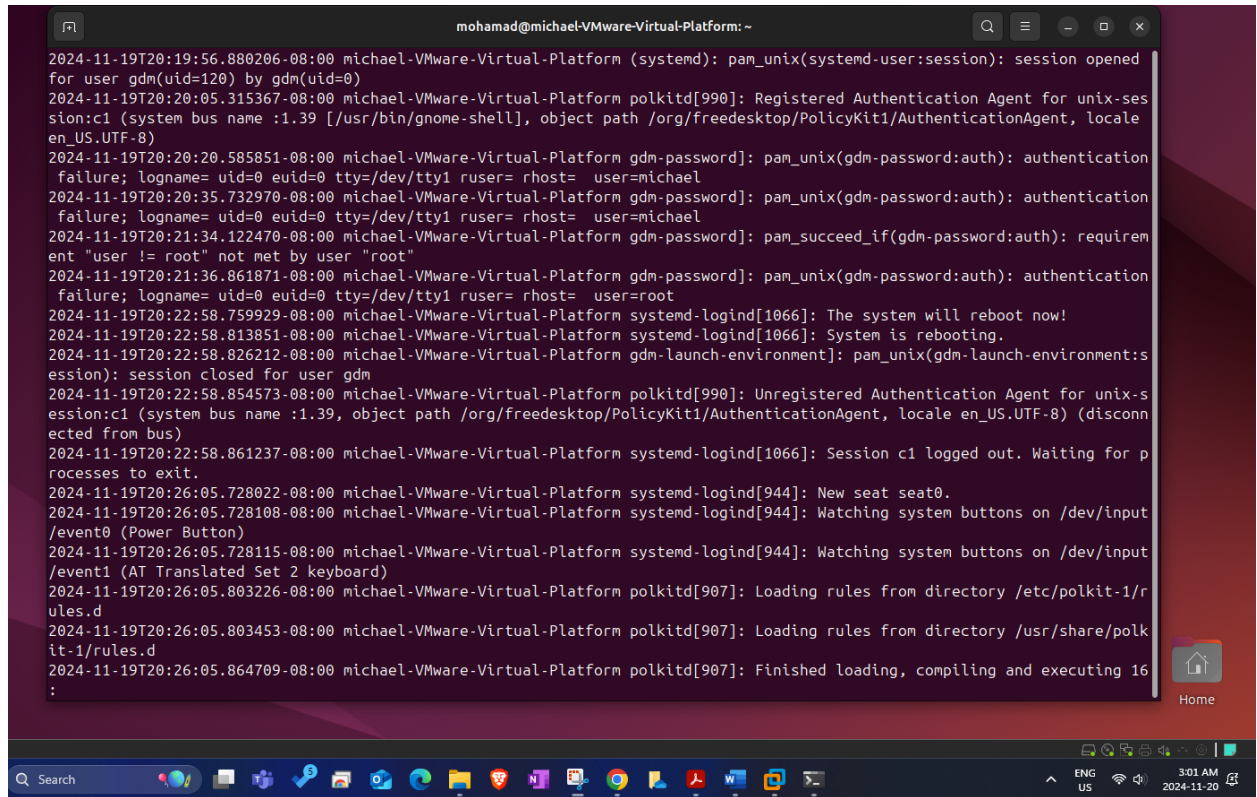


Monitor Logs

Benefit: Helps detect unusual activity by reviewing system logs.



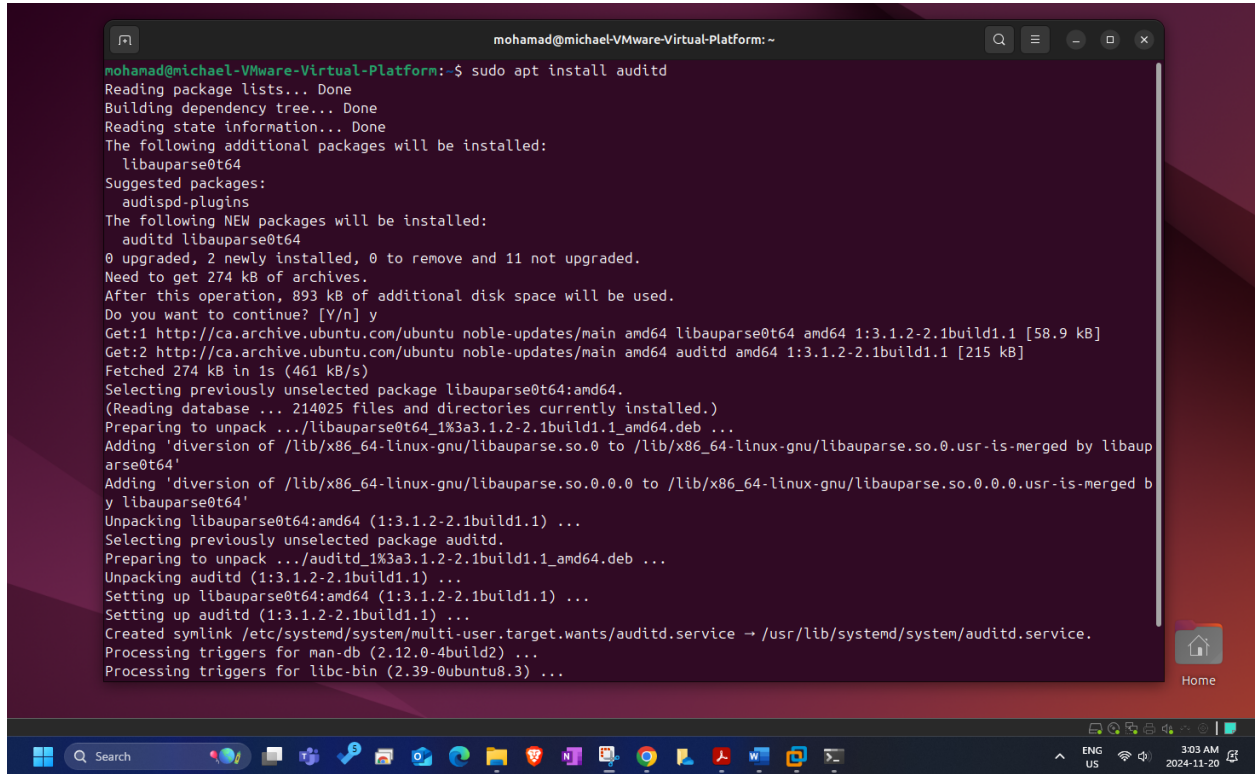
```
mohamad@michael-VMware-Virtual-Platform: ~  
mohamad@michael-VMware-Virtual-Platform:~$ sudo apt install logwatch  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  libdate-manip-perl libnsl2 postfix  
Suggested packages:  
  libsys-cpu-perl libsys-meminfo-perl mail-reader postfix-cdb postfix-doc postfix-ldap postfix-lmdb  
  postfix-mta-sts-resolver postfix-mysql postfix-pcre postfix-pgsql postfix-sqlite procmail sasl2-bin | dovecot-common  
The following NEW packages will be installed:  
  libdate-manip-perl libnsl2 logwatch postfix  
0 upgraded, 4 newly installed, 0 to remove and 11 not upgraded.  
Need to get 2,606 kB of archives.  
After this operation, 18.5 MB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 libnsl2 amd64 1.3.0-3build3 [41.4 kB]  
Get:2 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 postfix amd64 3.8.6-1build2 [1,254 kB]  
Get:3 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 libdate-manip-perl all 6.95-1 [923 kB]  
Get:4 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 logwatch all 7.7-1ubuntu1 [388 kB]  
Fetched 2,606 kB in 2s (1,517 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package libnsl2:amd64.  
(Reading database ... 212529 files and directories currently installed.)  
Preparing to unpack .../libnsl2_1.3.0-3build3_amd64.deb ...  
Unpacking libnsl2:amd64 (1.3.0-3build3) ...  
Selecting previously unselected package postfix.  
Preparing to unpack .../postfix_3.8.6-1build2_amd64.deb ...  
Unpacking postfix (3.8.6-1build2) ...  
Selecting previously unselected package libdate-manip-perl.  
Preparing to unpack .../libdate-manip-perl_6.95-1_all.deb ...  
Unpacking libdate-manip-perl (6.95-1) ...  
Selecting previously unselected package logwatch.  
Preparing to unpack .../logwatch_7.7-1ubuntu1_all.deb ...
```



```
mohamad@michael-VMware-Virtual-Platform: ~  
2024-11-19T20:19:56.880206-08:00 michael-VMware-Virtual-Platform (systemd): pam_unix(systemd-user:session): session opened  
for user gdm(uid=120) by gdm(uid=0)  
2024-11-19T20:20:05.315367-08:00 michael-VMware-Virtual-Platform polkitd[990]: Registered Authentication Agent for unix-ses  
sion:c1 (system bus name :1.39 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale  
en_US.UTF-8)  
2024-11-19T20:20:20.585851-08:00 michael-VMware-Virtual-Platform gdm-password]: pam_unix(gdm-password:auth): authentication  
failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=michael  
2024-11-19T20:20:35.732970-08:00 michael-VMware-Virtual-Platform gdm-password]: pam_unix(gdm-password:auth): authentication  
failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=michael  
2024-11-19T20:21:34.122470-08:00 michael-VMware-Virtual-Platform gdm-password]: pam_succeed_if(gdm-password:auth): requirem  
ent "user != root" not met by user "root"  
2024-11-19T20:21:36.861871-08:00 michael-VMware-Virtual-Platform gdm-password]: pam_unix(gdm-password:auth): authentication  
failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=root  
2024-11-19T20:22:58.759929-08:00 michael-VMware-Virtual-Platform systemd-logind[1066]: The system will reboot now!  
2024-11-19T20:22:58.813851-08:00 michael-VMware-Virtual-Platform systemd-logind[1066]: System is rebooting.  
2024-11-19T20:22:58.826212-08:00 michael-VMware-Virtual-Platform gdm-launch-environment]: pam_unix(gdm-launch-environment:s  
ession): session closed for user gdm  
2024-11-19T20:22:58.854573-08:00 michael-VMware-Virtual-Platform polkitd[990]: Unregistered Authentication Agent for unix-s  
ession:c1 (system bus name :1.39, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconn  
ected from bus)  
2024-11-19T20:22:58.861237-08:00 michael-VMware-Virtual-Platform systemd-logind[1066]: Session c1 logged out. Waiting for p  
rocesses to exit.  
2024-11-19T20:26:05.728022-08:00 michael-VMware-Virtual-Platform systemd-logind[944]: New seat seat0.  
2024-11-19T20:26:05.728108-08:00 michael-VMware-Virtual-Platform systemd-logind[944]: Watching system buttons on /dev/input  
/event0 (Power Button)  
2024-11-19T20:26:05.728115-08:00 michael-VMware-Virtual-Platform systemd-logind[944]: Watching system buttons on /dev/input  
/event1 (AT Translated Set 2 keyboard)  
2024-11-19T20:26:05.803226-08:00 michael-VMware-Virtual-Platform polkitd[907]: Loading rules from directory /etc/polkit-1/r  
ules.d  
2024-11-19T20:26:05.803453-08:00 michael-VMware-Virtual-Platform polkitd[907]: Loading rules from directory /usr/share/pol  
kit-1/rules.d  
2024-11-19T20:26:05.864709-08:00 michael-VMware-Virtual-Platform polkitd[907]: Finished loading, compiling and executing 16  
:  
Home
```

Enable Auditing

Benefit: Tracks system activities to detect suspicious behavior or unauthorized changes.



The screenshot shows a terminal window titled "mohamad@michael-VMware-Virtual-Platform: ~". The user has executed the command "sudo apt install auditd". The terminal output shows the package lists being read, the dependency tree being built, and the state information being read. It then lists the additional packages to be installed: libauparse0t64 and audispd-plugins. The user is prompted to continue, and they press 'y'. The terminal then shows the packages being fetched from the Ubuntu archive, unpacked, and installed. It also shows the creation of a symlink for the auditd service and the processing of triggers for man-db and libc-bin.

```
mohamad@michael-VMware-Virtual-Platform: ~$ sudo apt install auditd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libauparse0t64
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd libauparse0t64
0 upgraded, 2 newly installed, 0 to remove and 11 not upgraded.
Need to get 274 kB of archives.
After this operation, 893 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ca.archive.ubuntu.com/ubuntu noble-updates/main amd64 libauparse0t64 amd64 1:3.1.2-2.1build1.1 [58.9 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu noble-updates/main amd64 auditd amd64 1:3.1.2-2.1build1.1 [215 kB]
Fetched 274 kB in 1s (461 kB/s)
Selecting previously unselected package libauparse0t64:amd64.
(Reading database ... 214025 files and directories currently installed.)
Preparing to unpack .../libauparse0t64_1%3a3.1.2-2.1build1.1_amd64.deb ...
Adding 'diversion of /lib/x86_64-linux-gnu/libauparse.so.0 to /lib/x86_64-linux-gnu/libauparse.so.0.usr-is-merged by libauparse0t64'
Adding 'diversion of /lib/x86_64-linux-gnu/libauparse.so.0.0.0 to /lib/x86_64-linux-gnu/libauparse.so.0.0.0.usr-is-merged by libauparse0t64'
Unpacking libauparse0t64:amd64 (1:3.1.2-2.1build1.1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a3.1.2-2.1build1.1_amd64.deb ...
Unpacking auditd (1:3.1.2-2.1build1.1) ...
Setting up libauparse0t64:amd64 (1:3.1.2-2.1build1.1) ...
Setting up auditd (1:3.1.2-2.1build1.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service -> /usr/lib/systemd/system/auditd.service.
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
```